УДК 004.56

А.А. БРЮХОВЕЦКИЙ, А.В. СКАТКОВ, П.О. БЕРЕЗЕНКО

Севастопольский национальный технический университет, Украина

ОБНАРУЖЕНИЕ УЯЗВИМОСТЕЙ В КРИТИЧЕСКИХ ПРИЛОЖЕНИЯХ НА ОСНОВЕ РЕШАЮЩИХ ДЕРЕВЬЕВ

Предложена модель обнаружения уязвимостей на основе решающих деревьев. Модель построена на исследования значений признаков сетевого трафика. Исходными данными для разрабатываемой модели служат данные представленные в базе данных KDD CUP'99, которые широко используются при разработке систем обнаружения вторжений (СОВ). Разрабатываемая система относится к СОВ, которая контролирует состояние трафика с целью определения аномалий – отклонений значений от нормального состояния. Применяемая в ней адаптивная технология позволяет обнаруживать новые виды атак. Основное внимание при разработке модели уделено выявлению наиболее информативных признаков сетевого трафика. Это позволяет существенно снизить размерность анализируемого пространства признаков, увеличить быстродействие, повысить точность обнаружения и снизить уровень ложных срабатываний. Представлено детальное описание признаков сетевого трафика и их классификация, описан метод построения решающего дерева на основе оценки энтропии подмножеств обрабатываемых данных, разработан алгоритм построения решающего дерева. Приведенные результаты экспериментальных исследований с программной моделью, показывают, что при контроле тестовых данных точность обнаружения вторжений (DR) достигает 98%.

Ключевые слова: *сетевой трафик, обнаружение уязвимостей, информационная безопасность, решающие деревья.*

Введение

В связи с интенсивным ростом информационных технологий и их внедрением в различные отрасли деятельности человека вопрос информационной безопасности становится все более актуальным. На сегодняшний день большинство организаций для защиты своих корпоративных сетей использует те или иные средства защиты от вторжений (межсетевые экраны, антивирусные системы и системы обнаружения вторжений). Системы обнаружения вторжений – это программные или аппаратно - программные средства, которые автоматизируют процесс контроля событий, протекающих в компьютерной системе или сети, и самостоятельно анализируют эти события в поисках признаков нарушения политики безопасности. Системы обнаружения вторжений (СОВ) на сегодняшний день являются одним из необходимых компонентов инфраструктуры безопасности информационных систем для большинства организаций [1 – 4].

В зависимости от источника обнаружения вторжений различают системы уровня host-based (HBIDS), сетевые СОВ (NIDS – network intrusion detection), а также системы уровня приложений (APIDS) и гибридные СОВ (HIDS), которые сочетают комбинированные методы [1]. Первые идентифицируют вторжения, анализируя события и трафик, поступающий на отдельный компьютер, в то время как вторые – исследуют сетевой трафик. Системы уровня приложений , как правило, располагаются между web-сервером и, например, SQL-сервером. На рис. 1 представлена структура компьютерной сети с альтернативным расположением СОВ.

В свою очередь, системы обнаружения вторжений, в зависимости от используемой технологии выявления атак, разделяют на два основных типа: системы обнаружения злоумышленного поведения и системы обнаружения аномального поведения.

Первые ориентируются на модель злонамеренного поведения (например, шаблон/сигнатура атаки) и сравнивают модель с потоком событий. На основании сравнительного анализа система принимает решение блокировать тот или иной пакет, либо пропускать для взаимодействия непосредственно с операционной системой. Сигнатурные системы обнаружения вторжений обладают высокой производительностью, эффективностью обнаружения при сравнительно невысоких требованиях к аппаратному обеспечению. Однако они имеют ряд недостатков: невозможность автоматического ввода новых сигнатур, отсутствие системы блокирования неизвестных сигнатур, отсутствие возможностей прогнозирования действий злоумышленника, отсутствие подсистемы мониторинга аппаратных ресурсов и другие. Существующие сигнатурные системы обна-

ружения вторжений не могут профилировать перехваченный поток данных распределенных вторжений для их классификации и выработки сигнала о вторжении. Поэтому системы обнаружения вторжений второго типа используют методы для распознавания неизвестных атак. Такие СОВ проектируются, как правило, на основе моделей нормального поведения (например, профиль системы) и ищут аномальные вхождения в поток событий.

Задача исследования нормального и аномального поведения сетевых компьютерных систем является очень сложной и комплексной. Для ее решения используются, как правило, различные статистические модели для оценки вероятности появления заданных значений (событий). Низкая и высокая вероятность в этом случае может означать появление аномалий.

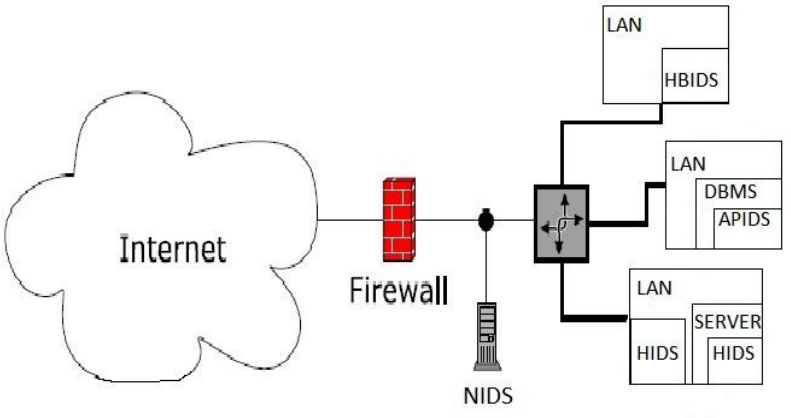

Рис. 1. Структура компьютерной сети с альтернативным расположением СОВ

Для сравнительного анализа методов обнаружения вторжений могут быть выбраны следующие критерии:

- уровень наблюдения за системой;
- верифицируемость метода (позволяет провести экспертную оценку корректности метода и его реализации в произвольный момент времени, в том числе в процессе эксплуатации системы обнаружения на его основе);
- адаптивность метода (устойчивость метода к малым изменениям реализации атаки, которые не изменяют результат атаки);
- точность обнаружения вторжений и уровень ложных тревог и др.

Несмотря на широкое распространение СОВ и активные исследования в данной области, существует потребность в разработке новых методов и моделей обнаружения сетевых атак.

Целью работы является разработка модели обнаружения вредоносных программ по значениям признаков в сетевом трафике на основе решающих деревьев. Разрабатываемая система относится к СОВ, которые обнаруживают аномальное состояние трафика, а значит применяемая в ней технология позволяет обнаруживать новые виды атак.

Постановка задачи исследования

Набор данных, который используется в работе для построения модели, был смоделирован и получен в компьютерной сети ВВС США с целью имитации компьютерных атак и содержится в базе данных лаборатории MIT Lincoln Labs [2]. Данные содержат около 4 Гб сжатого TCP сетевого трафика, который собирался 7 недель и составил около 5 миллионов записей о соединениях. Каждое TCP / IP соединение состоит из 41 количественного и качественного признака. Последний 42-й признак характеризует состояние трафика. Оно может быть нормальным или аномальным. Каждая запись содержит около 100 байт. Признаки могут быть разделены на три группы:

- основные характеристики соединения, например, продолжительность соединения, тип протокола, сервис, число переданных байт от источника к приемнику и в обратном направлении, отдельные флаги (табл. 1). Некоторые значения признаков определяются с задержкой в течение определенного временного интервала;
- статистические характеристики трафика, которые вычисляются с использованием 2-х секундного временного окна или в течении большего временного промежутка (табл. 2). Характеристики подразделяются на две группы: атрибуты относящиеся к конкретному host – компьютеру или к конкретному сервису. Отдельные атаки сканирования портов выполняются дольше, чем 2 сек. Поэтому ряд признаков обрабатывается окном в 100 соединений;
- признаки внутри отдельного соединения (табл. 3). В отличие от большинства DoS – атак и

сканирования портов, R2L и R2U атаки характеризуются отдельными непродолжительными проявлениями к отдельному компьютеру. В то время как DoS – атаки и Probing инициируют множественные соединения в короткий промежуток времени.

В таблицах 1 – 3 приведены группы признаков сетевого трафика.

Таблица 1

Основные признаки

Признак	Тип
duration	continuous
protocol_type	discrete
service	discrete
number of data bytes source-destination	continuous
number of data bytes destination-source	continuous
flag status	discrete
land	discrete
wrong_fragment	discrete
urgent packets	discrete

Таблица 2

Статистические признаки

Признак	Тип
count	continuous
serror_rate	continuous
rerror_rate	continuous
same_srv_rate	continuous
diff_srv_rate	continuous
srv_count	continuous
srv_serror_rate	continuous
srv_rerror_rate	continuous
srv_diff_host_rate	continuous

Таблица 3

Признаки отдельного соединения

Признак	Тип
hot	continuous
num_failed_logins	continuous
logged_in	discrete
num_compromised	continuous
root_shell	discrete
su_attempted	discrete
num_root	continuous
num_file_creations	continuous
num_shells	continuous
num_access_files	continuous
num_outbound_cmds	continuous
is_hot_login	discrete
is_guest_login	discrete

Более подробная информация о признаках сетевого трафика может быть получена в [2]. На основе приведенных данных требуется построить дерево классификации.

Метод решения задачи

Пусть задано множество примеров T, где каждый элемент этого множества описывается m атрибутами. Количество примеров в множестве T будем называть мощностью этого множества и будем обозначать |T|. Метка класса C принимает следующие значения C_1, C_2 … C_k. Пусть $freq(C_j,T)$ – количество примеров из множества T, относящихся к одному и тому же классу C_j. Тогда выражение

$$\text{Info}(T) = -\sum_{j=1}^{k} \frac{\text{freq}(C_j, T)}{|T|} \log_2 \left(\frac{\text{frec}(C_j, T)}{|T|} \right) \qquad (1)$$

дает оценку среднего количества информации. В терминологии теории информации данное выражение называется энтропией множества T. Ту же оценку, но только уже после разбиения множества T по атрибуту X на n подмножеств, дает следующее выражение:

$$\text{Info}_x(T) = \sum_{i=1}^{n} \frac{|T_i|}{|T|} \text{Info}(T_i). \qquad (2)$$

Критерий оценки значения энтропии до и после разбиения – прирост информации, рассчитывается по следующей формуле:

$$\text{Gain}(X) = \text{Info}(T) - \text{Info}_x(T). \qquad (3)$$

Далее вводится нормализация по формуле:

$$\text{Split\_Info}_x(T) = -\sum_{i=1}^{n} \frac{T_i}{T} \log_2 \left(\frac{T_i}{T} \right). \qquad (4)$$

Выражение (4) оценивает потенциальную информацию, получаемую при разбиении множества T на n подмножеств. Основная задача – определить значение признака, по которому будет происходить разбиение исходного множества. Для этого используется критерий Gain_Ratio, который вычисляется по формуле (5):

$$\text{Gain\_Ratio}(X) = \text{Gain}(X) / \text{Split\_Info}_x(T). \qquad (5)$$

Алгоритм построения дерева классификаций.

1. Выбрать i атрибут, где $i \in [1; m]$.

2. Упорядочить значения атрибута по возрастанию.

3. Создать множество всех возможных точек разбиения для атрибута X.

4. Для полученных точек разбиения вычисляем прирост информации gain и потенциальную информацию, получаемую при разбиении множества T на n подмножеств – *split_Info.*

5. Вычисляем значение критерия gain_ratio для всех возможных полученных точек разбиения.

6. Выбираем границу разделения, для которой критерий gain_ratio = Max.

7. Повторяем п.п.1 – 6 для каждого из полученных подмножеств, пока листья дерева не будут содержать образцы одного класса.

8. Конец (сформирована система правил).

Результаты экспериментальных исследований

Модель системы обнаружения вторжения реализована в программной среде – Eclipse. Занимаемый обьем 2,3 мБ памяти. В результате исследования программной системы были получены основные характеристики. Эксперименты проводились на смешанной (нормальной и аномальной) обучающей и тестовой выборках данных базы KDD. Время обучения на представленных данных занимает 38 минут. Тестовая выборка проверялась по 14 числовым атрибутам сетевого трафика, которые были определены, как оптимальные, после обучения модели.

Полученные в результате моделирования признаки, отобранные для классификации представлены в табл. 4.

Таблица 4

Классификационные признаки

Номер атрибута	Имя атрибута
1	duration
5	src_bytes
6	dst_bytes
23	Count
24	srv_count
29	same_srv_rate
32	dst_host_count
33	dst_host_srv_count
34	dst_host_same_srv_rate
35	dst_host_diff_srv_rate
36	dst_host_same_src_port_rate
38	dst_host_serror_rate
39	dst_host_srv_serror_rate
40	dst_host_rerror_rate

Атрибуты 23 и 24 имеют наибольшее значение критерия расщепления Gain_Ratio по сравнению с другими атрибутами.

В табл. 5 приведено количество записей обучающей и тестовой выборок, принадлежащих конкретным классам.

Характеристики точности и уровня ложных срабатываний представлены в табл. 6.

Выражения для определения этих характеристик приведены ниже [3, 4]:

Таблица 5

Число обучающих и тестовых записей

Классы данных	Обучающая выборка	Тестирующая выборка
Normal	107273	90592
DoS	441458	572594
R2L	1126	7683
U2R	52	70
Probing	3157	4189
Всего	553006	675128

Таблица 6

Характеристики СОВ

	Normal	Probe	DOS	U2R	R2L
DR(%)	98,03	92,75	97,76	68,23	79,21
FAR (%)	0,3	5,43	1,27	7,32	9,41

DR – частота выявления атаки

$$DR= TP/(TP+FN) \quad (6)$$

и FAR – уровень ложной тревоги (False Alarm,):

$$FAR=FP/(FP+TN), \quad (7)$$

где TP (true positive) – количество правильно классифицированных аномалий, FN (false negative) – количество образцов нормального трафика определенного системой как аномальный, FP (false positive) – количество аномальных образцов сетевого трафика определенных системой как нормальные, TN (true negative) – количество правильно идентифицированных системой образцов нормального трафика.

Указанные параметры позволяют оценить число правильно обнаруженных нормальных и аномальных образцов, а также — ошибки первого и второго рода.

Заключение

Предложена модель обнаружения вредоносных программ на основе решающих деревьев. Модель построена на исследования значений признаков сетевого трафика. Разрабатываемая система контролирует аномалии в сетевом трафике. Применяемая в ней адаптивная технология позволяет обнаруживать новые виды атак. Основное внимание при разработке модели уделено выявлению наиболее информативных признаков сетевого трафика. Это позволяет существенно снизить размерность анализируемого пространства признаков, увеличить быстродействие, повысить точность обнаружения и снизить уровень ложных срабатываний.

Целью дальнейших исследований является использование информативных признаков в моделях обнаружения вредоносных программ, построенных на основе нечеткой логики, негативной селекции,

искусственных иммунных систем и других. Интерес представляют модели, построенные на основе комбинированных методов обнаружения уязвимостей.

Литература

1. Искусственные иммунные системы и их применение [Текст] / Под ред. Д. Дасгупты. Пер. с англ. – М.: Физматлит, 2006. – 344 с.

2. KDD cup 99 Intrusion detection data set [Электронный ресурс]. – Электронные текстовые данные (752 Мб). – Darpa: Irvine, CA 92697-3425, 1999. – Режим доступа к ресурсу: http: // kdd.ics.uci.edu/databases/kddcup99/kddcup/task.html. – Monday, 17 March 2013 19:07:34.

3. Dasgupta, D. MILA – Multilevel Immune Learning Algorithm [Текст] / D. Dasgupta, S. Yu, N. Majumdar // Proceedings of the Genetic and Evolutionary Computation Conference – 2003. – Springer – Verlag: Berlin Heidelberg, 2003. – P. 183 – 194.

4. Ji, Z. Real-valued negative selection algorithm with variable-sized detectors [Текст] / Z. Ji, D. Dasgupta // Proceedings of the Genetic and Evolutionary Computation – 2004. – Springer – Verlag: Seattle, WA, USA ,2004. – P. 287 – 298.

Поступила в редакцию 28.02.2013, рассмотрена на редколлегии 27.03.2013

Рецензент: д-р техн. наук, проф., проф. кафедры технической кибернетики Л.А. Краснодубец, Севастопольский национальный технический университет, Севастополь, Украина.

ВИЯВЛЕННЯ УРАЗЛИВОСТЕЙ В КРИТИЧНИХ ДОДАТКІВ НА ОСНОВІ ВИРІШАЛЬНИХ ДЕРЕВ

О.О. Брюховецький, О.В. Скатков, П.О. Березенко

Запропоновано модель виявлення уразливості на основі вирішальних дерев. Модель побудована на дослідженні значень ознак мережевого трафіка. Вихідними даними для розробленої моделі є дані, представлені в базі даних KDD CUP'99, які широко використовуються при розробці систем виявлення вторгнень (СВВ). Розроблена система відноситься до СВВ, яка контролює стан трафіка з метою визначення аномалій – відхилень значень від нормального стану. Основна увага при розробці моделі приділена виявленню найбільш інформативних ознак мережевого трафіка. Це дозволяє істотно знизити розмірність аналізованого простору ознак, збільшити швидкодію, підвищити точність виявлення і знизити рівень помилкових спрацьовувань. Представлено детальний опис ознак мережевого трафіка і їх класифікація, описаний метод побудови вирішального дерева на основі оцінки ентропії підмножин оброблюваних даних, розроблено алгоритм побудови вирішального дерева. Наведені результати експериментальних досліджень з програмної моделлю показують, що при контролі тестових даних точність виявлення вторгнень (DR) досягає 98%.

Ключові слова: мережевий трафік, виявлення уразливість, інформаційна безпека, вирішальні дерева.

DETECTION OF VULNERABILITIES IN CRITICAL APPLICATIONS BASED ON DECISION TREES

A.A. Bryukhovetskiy, A.V. Skatkov, P.O. Berezenko

A model of vulnerabilities detection based on decision trees was suggested. Model is based on the study of feature values of network traffic. Initial data for the developed model is the data submitted to the database KDD CUP'99, which are widely used in the development of intrusion detection systems. Intrusion detection systems (IDS) are today an essential component of the infrastructure of information systems security for most organizations. The developed system belongs to the IDS, which monitors the traffic in order to identify anomalies - deviations from normal values. The focus is in developing the model on identifying the most informative features of network traffic. This can significantly reduce the dimension of the space of the analyzed features, increase performance, increase the detection accuracy and reduce false positives. It's presented a detailed description of the characteristics of network traffic and their classification, for the method to build a decision tree based on the evaluation of the entropy of subsets of data to be processed, the algorithm of constructing a decision tree. The presented results of experimental studies with the programming model show that in the control test data accuracy of intrusion detection (DR) is 98%.

Key words: network traffic, vulnerabilities, intrusion detection, information security, decision trees.

Брюховецкий Алексей Алексеевич – канд. техн. наук, доцент, доцент кафедры кибернетики и вычислительной техники Севастопольского национального технического университета, Севастополь, Украина, e-mail: a.alexir@mail.ru.

Скатков Александр Владимирович – д-р техн. наук, профессор, профессор кафедры кибернетики и вычислительной техники Севастопольского национального технического университета, Севастополь, Украина, e-mail: kvt.sevntu@gmail.com.ua.

Березенко Павел Олегович – магистрант кафедры кибернетики и вычислительной техники Севастопольского национального технического университета, Севастополь, Украина.